UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

NISSIM RAM, on behalf of himself and all others similarly situated, Plaintiff, v. NEW YORK UNIVERSITY, Defendant.	Case No.: 1:25-cv-2510 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Nissim Ram ("Plaintiff") brings this Class Action Complaint ("Complaint") against New York University ("NYU") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF ACTION

1. Plaintiff brings this class action against Defendant for its failure to adequately secure and protect the sensitive personal information of its students and student applicants.

2. NYU is a private university located in New York, New York.

3. Plaintiff and Class Members entrusted NYU with their sensitive personal information under the mutual understanding that it would be safeguarded against unauthorized access. However, due to the Data Breach, this information was unlawfully accessed, compromised, and exposed.

4. NYU collected and maintained certain personally identifiable information of Plaintiff and the putative Class Members (defined below), who are current or former students or student applicants at Defendant's institution.

5. The PII compromised in the Data Breach included Plaintiff's and Class Members'

full names, test scores, majors, cities and zip codes, student applications, demographic data, and citizenship statuses ("PII").

6. The PII compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target PII for its value to identity thieves.

7. As a result of the Data Breach, Plaintiff and Class Members suffered concrete and actual injuries, including but not limited to:

(i) Invasion of privacy;
(ii) Theft and unauthorized access to their PII;
(iii) Diminished value of their PII;
(iv) Lost time and opportunity costs incurred while mitigating the consequences of the Data Breach;
(v) Loss of the benefit of their bargain;
(vi) Financial and opportunity costs associated with ongoing mitigation efforts;
(vii) Nominal damages; and
(viii) The continued and significantly heightened risk of future harm, because their PII:
(a) Remains unencrypted and accessible to unauthorized third parties; and
(b) Continues to be stored and backed up by Defendant without adequate safeguards, leaving it vulnerable to further unauthorized disclosures.

8. The Data Breach was a direct result of NYU's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect consumers' PII from a foreseeable and preventable cyber-attack.

9. Moreover, NYU was targeted for a cyber-attack due to its status as an educational institutions company that collects and maintains highly valuable PII on its systems.

10. NYU maintained, used, and shared the PII in a reckless manner. In particular, the PII was used and transmitted by Defendant in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

11. NYU disregarded the rights of Plaintiff and Class Members by, among other things, intentionally, willfully, recklessly, or negligently failing to implement adequate and reasonable measures to secure its data systems against unauthorized access; neglecting to take standard, readily available precautions to prevent the Data Breach; and failing to provide Plaintiff and Class Members with timely and accurate notice of the breach.

12. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained has been accessed and acquired by data thieves.

13. With the PII obtained in the Data Breach, data thieves have already engaged in identity theft and fraud and can continue to perpetrate various crimes, including but not limited to: opening new financial accounts in Class Members' names, taking out fraudulent loans, using stolen information to claim government benefits, filing fraudulent tax returns, obtaining driver's licenses with false identities, and providing law enforcement with false information during an arrest.

14. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

15. Plaintiff and Class Members may also incur out-of-pocket expenses for protective measures, such as credit monitoring services, credit freezes, credit reports, and other safeguards to detect and prevent identity theft.

16. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

17. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach.

18. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and members of the proposed Class, including Plaintiff, are citizens of states different from Defendant.

20. This Court has jurisdiction over Defendant through its business operations in this District, the specific nature of which occurs in this District. Defendant's principal place of business is in this District. Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is located in this District and a substantial part of the events and omissions giving rise to this action occurred in this District.

PARTIES

22. Plaintiff Nissim Ram is a resident and citizen of New York, New York.

23. Defendant New York University is a university with its headquarters and principal place of business located in New York, New York.

FACTUAL ALLEGATIONS

24. NYU is a private university based in New York, New York.

25. Plaintiff and Class Members are current and former students and student-applicants

of NYU.

26. Throughout their relationship with NYU, students and student applicants, including Plaintiff and Class Members, entrusted the university with their sensitive PII.

27. In collecting PII from students and student applicants, including Plaintiff, NYU expressly represented—through its privacy policy and other disclosures made in compliance with statutory privacy requirements—that it would maintain the confidentiality and security of the data it collected.

28. Indeed, NYU provides on its website that: "New York University (NYU) is committed to respecting your privacy."[1]

29. Plaintiff and the Class Members, as students or student-applicants at NYU, relied on these promises and on this sophisticated business entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Consumers, in general, demand security to safeguard their PII.

The Data Breach

30. In or around March 2025, a hacker reportedly took control of NYU's website for at least two hours on a Saturday morning, exposing the names, test scores, intended majors, and zip codes of over three million applicants. The breach also compromised information about their family members and financial aid records dating back to at least 1989.[2]

31. At approximately 10:30 a.m., a Reddit user reported a compromised webpage that exposed four publicly accessible CSV files containing sensitive NYU admissions data dating back to at least 1989. The files revealed information on over three million admitted students, including application details, demographic data, city and zip codes, and citizenship status. Additionally, the

[1] https://www.nyu.edu/footer/privacy.html.
[2] https://nyunews.com/news/2025/03/22/nyu-website-hacked-data-leak/

files contained Common Application data, such as financial aid records, statistics on rejected applicants, Early Decision data, and personal details about students' siblings and parents.[3]

32. NYU had a legal obligation under the FTC Act, contract law, common law, and industry standards to maintain the confidentiality of Plaintiff's and Class Members' PII and to safeguard it from unauthorized access and disclosure.

33. NYU did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

34. The attacker accessed and acquired files containing unencrypted PII of Plaintiff and Class Members. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

35. Plaintiff further believes that his PII and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Preventing Data Breaches: A Necessity, Not an Option.

36. NYU failed to implement reasonable security measures and practices suitable for safeguarding the sensitive information of Plaintiff and Class Members, leading to the exposure of Personally Identifiable Information (PII). This failure included a lack of encryption and proper data retention protocols, such as deleting information when no longer necessary.

37. NYU could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

38. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[4]

---

[3] *Id.*

[4] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

39. To prevent and detect cyber-attacks and ransomware incidents, NYU could and should have implemented, as recommended by the United States Government, the following security measures:

- Implement an awareness and training program: Since end users are common targets, employees and individuals should be trained to recognize ransomware threats and understand how they are delivered.
- Enable strong spam filters: Prevent phishing emails from reaching end users and authenticate inbound emails using technologies such as Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to block email spoofing.
- Scan all incoming and outgoing emails: Detect potential threats and filter out executable files from reaching end users.
- Configure firewalls to block malicious IP addresses: Restrict access from known sources of malicious activity.
- Patch systems regularly: Ensure operating systems, software, and firmware are updated through a centralized patch management system.
- Automate anti-virus and anti-malware scans: Set these programs to conduct regular, automated scans to detect potential threats.
- Manage privileged accounts based on the principle of least privilege: Limit administrative access to only those who absolutely need it, and restrict the use of these accounts to necessary tasks.
- Set access controls with least privilege in mind: Ensure users can only access files, directories, or network shares they need for their role—avoiding unnecessary write permissions.
- Disable macros in email-transmitted Office files: Consider using Office Viewer software instead of full applications to open files sent via email, preventing harmful macros from executing.
- Implement Software Restriction Policies (SRP): Prevent programs from executing from common ransomware locations, such as temporary folders used by web browsers or compression programs, including the AppData/LocalAppData folder.
- Disable Remote Desktop Protocol (RDP) when not in use: Minimize attack surfaces by turning off RDP if it's unnecessary.
- Use application whitelisting: Only permit known, authorized programs to execute on systems, enhancing control over what runs on the network.

- Run critical programs in virtualized environments: Isolate potentially vulnerable programs in secure, controlled environments to minimize risk.

- Categorize data based on organizational value: Implement physical and logical network separation to protect sensitive data across different organizational units.[5]

40. To prevent and detect cyber-attacks or ransomware attacks, NYU could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection

[5] *See Id.* at 3-4.

- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[6]

41. Given that NYU was storing the PII of its current and former students and student-applicants, NYU could and should have implemented all of the above measures to prevent and detect cyberattacks.

42. The occurrence of the Data Breach indicates that NYU failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the PII of, upon information and belief, more than three million individuals, including that of Plaintiff and Class Members.

NYU Acquires, Collects, And Stores Its Students and Student-Applicants' PII

43. NYU acquires, collects, and stores a massive amount of PII on its current and former students and student-applicants.

44. As a condition of applying for enrollment at NYU, it requires that students and student-applicants and other personnel entrust it with highly sensitive personal information.

45. By obtaining, collecting, and using Plaintiff's and Class Members' PII, NYU assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

46. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and would not have entrusted it to NYU absent a promise to safeguard that information.

47. Upon information and belief, in the course of collecting PII from students and student-applicants, including Plaintiff, NYU promised to provide confidentiality and adequate

[6] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a- preventable-disaster/

security for their data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

48. Plaintiff and the Class Members relied on NYU to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

NYU Was Aware, or Should Have Been Aware, of the Risk Due to the Increased Vulnerability of Educational Institutions Holding PII to Cyber Attacks

49. NYU's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting educational institutions that collect and store PII, like NYU, preceding the date of the breach.

50. Data breaches, including those perpetrated against educational institutions that store PII in their systems, have become widespread.

51. In light of recent high profile data breaches at other industry leading companies, including National Public Data (2.9 billion records, August 2024), Ticketmaster Entertainment, LLC (560 million records, May 2024), Change Healthcare Inc. (145 million records, February 2024), Dell Technologies, Inc. (49 million records, May 2024), and AT&T Inc. (73 million records, April 2024), NYU knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

52. The injuries to Plaintiff and Class Members were directly and proximately caused by NYU's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

53. The ramifications of NYU's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

54. As an educational institutions company in custody of the PII of its students and

student-applicants, NYU knew, or should have known, the importance of safeguarding PII entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. NYU failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value Of PII

55. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[7] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[8]

56. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[9]

57. For example, Personal Information can be sold at a price ranging from $40 to $200.[10] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[11]

58. Based on the foregoing, the information compromised in the Data Breach is

[7] 17 C.F.R. § 248.201 (2013).
[8] *Id.*
[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark- web-how-much-it-costs/
[10] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your- personal-information-is-selling-for-on-the-dark-web/
[11] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

59. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[12]

60. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

61. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[13]

62. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

NYU Fails to Comply with FTC Guidelines

63. The Federal Trade Commission ("FTC") has promulgated numerous guides for

[12] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x- price-of-stolen-credit-card-numbers.html.

[13] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf

businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

64. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[14]

65. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

66. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

67. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to

[14] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).

meet their data security obligations.

68. These FTC enforcement actions include actions against educational institutions, like NYU.

69. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as NYU, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of NYU's duty in this regard.

70. NYU failed to properly implement basic data security practices.

71. NYU's failure to employ reasonable and appropriate measures to protect against unauthorized access to the PII of its students and student-applicants or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

72. Upon information and belief, NYU was at all times fully aware of its obligation to protect the PII of its students and student-applicants, NYU was also aware of the significant repercussions that would result from its failure to do so. Accordingly, NYU's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

NYU Fails to Comply with Industry Standards

73. As noted above, experts studying cyber security routinely identify Educational institutions in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

74. Several best practices have been identified that, at a minimum, should be implemented by Educational institutions in possession of PII, like NYU, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus,

and anti-malware software; encryption, making data unreadable without a key; multi- factor authentication; backup data and limiting which employees can access sensitive data. NYU failed to follow these industry best practices, including a failure to implement multi- factor authentication.

75. Other best cybersecurity practices that are standard for Educational institutions include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. NYU failed to follow these cybersecurity best practices, including failure to train staff.

76. NYU failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

77. These foregoing frameworks are existing and applicable industry standards for Educational institutions, and upon information and belief, NYU failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries & Damages

78. As a result of NYU's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy;

(ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in NYU's possession and is subject to further unauthorized disclosures so long as NYU fails to undertake appropriate and adequate measures to protect the PII.

Data Breaches Increase Victims' Risk of Identity Theft

79. The unencrypted PII of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

80. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Simply put, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

81. The connection between a data breach and the risk of identity theft is clear and well-established. When criminals gain access to PII, they steal it with the intent to profit. This stolen data is typically sold on the black market to other criminals, who then use it to carry out a range of identity theft-related crimes, as outlined below.

82. Plaintiff's and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

83. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[15]

[15] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the

84. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

85. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

86. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiff and the other Class Members.

87. Thus, even if certain information (such as contact information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

88. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate Risk of Identity Theft & Fraud

89. As a result of the recognized risk of identity theft, when a Data Breach occurs, and

---

dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-fro-texas-life-insurance (https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground- stolen-from-texas-life-insurance-finn/

an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

90. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach. Accordingly, the Data Breach has caused Plaintiff and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

91. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[16]

92. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[17]

Diminution of Value of PII

93. PII is a valuable property right.[18] Its value is axiomatic, considering the value of Big

[16] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[17] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps
[18] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007,

Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

94. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[19]

95. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[20]

96. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[21]

97. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[22]

98. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

99. At all relevant times, NYU knew, or reasonably should have known, of the

---

https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

[19] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.")

[20] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

[21] https://datacoup.com/

[22] https://digi.me/what-is-digime/

importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if NYU's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

100. The fraudulent activity resulting from the Data Breach may not come to light for years.

101. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

102. NYU was, or should have been, fully aware of the unique type and the significant volume of data on NYU's network, amounting to, upon information and belief, more than three million individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

103. The injuries to Plaintiff and Class Members were directly and proximately caused by NYU's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Reasonable and Essential: The Future Costs of Credit and Identity Theft Monitoring

104. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of PII involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes–*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

105. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her PII was used to file for unemployment

benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

106. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

107. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from NYU's Data Breach.

Loss of Benefit of The Bargain

108. Furthermore, NYU's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. When applying for enrollment at NYU under certain terms, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the enrollment services and necessary data security to protect the PII, when in fact, NYU did not provide the expected data security. Accordingly, Plaintiff and Class Members received enrollment services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with NYU.

Plaintiff's Experience

109. Plaintiff has been a graduate student at NYU since September 2024. As part of its standard business operations, NYU collected and maintained Plaintiff's PII.

110. Upon information and belief, at the time of the Data Breach, NYU maintained Plaintiff's PII in its system.

111. Plaintiff is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to NYU had he known of NYU's lax data security policies.

112. Upon information and belief, Plaintiff's PII was improperly targeted, accessed, and obtained by unauthorized third parties in the Data Breach.

113. As a result of the Data Breach, Plaintiff took reasonable steps to mitigate its impact, including researching and verifying its legitimacy. Plaintiff has spent significant time addressing the consequences of the breach—valuable time that otherwise would have been dedicated to work, recreation, and other pursuits. This lost time is irretrievable.

114. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in NYU's possession and is subject to further unauthorized disclosures so long as NYU fails to undertake appropriate and adequate measures to protect the PII.

115. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that NYU has still not fully informed Plaintiff of key details about the Data Breach's occurrence.

116. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

117. Also, as a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

118. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in NYU's possession, is protected and safeguarded from future

breaches.

CLASS ALLEGATIONS

119. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated, pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5).

120. The Class that Plaintiff seeks to represent is defined as follows:

> **All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by NYU in March 2025 (the "Class").**

121. Excluded from the Class are the following individuals and/or entities: NYU and NYU's parents, subsidiaries, affiliates, officers and directors, and any entity in which NYU have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

122. Plaintiff reserves the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

123. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiff and exclusively in the possession of NYU, upon information and belief, millions of individuals were impacted. The Class is apparently identifiable within NYU's records, and NYU has already identified these individuals (as evidenced by sending them breach notification letters).

124. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the

questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent NYU had a duty to protect the PII of Plaintiff and Class Members;

b. Whether NYU had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether NYU had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether NYU failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when NYU actually learned of the Data Breach;

f. Whether NYU adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether NYU violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether NYU failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether NYU adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages and/or nominal damages as a result of NYU's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

125. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

126. Policies Generally Applicable to the Class: This class action is also appropriate for certification because NYU acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct

toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. NYU's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on NYU's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

127. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intend to prosecute this action vigorously.

128. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like NYU. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

129. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because NYU would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of

individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

130. The litigation of the claims brought herein is manageable. NYU's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

131. Adequate notice can be given to Class Members directly using information maintained in NYU's records.

132. Unless a Class-wide injunction is issued, NYU may continue in its failure to properly secure the PII of Class Members, NYU may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and NYU may continue to act unlawfully as set forth in this Complaint.

133. Further, NYU has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

134. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether NYU failed to timely notify the Plaintiff and the class of the Data Breach;

b. Whether NYU owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether NYU's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether NYU's failure to institute adequate protective security measures amounted to negligence;

e. Whether NYU failed to take commercially reasonable steps to safeguard consumer PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

135. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

136. NYU requires its students and student-applicants, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of providing its services.

137. NYU gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to its students and student-applicants, which solicitations and services affect commerce.

138. Plaintiff and Class Members entrusted NYU with their PII with the understanding that NYU would safeguard their information.

139. NYU had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

140. By voluntarily undertaking and assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, NYU had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. NYU's duty included a responsibility to implement processes by which they could detect a breach

of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

141. NYU had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

142. NYU owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks adequately protected the PII.

143. NYU's duty of care to use reasonable security measures arose as a result of the special relationship that existed between NYU and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted NYU with their confidential PII, a necessary part of being students and/or student-applicants at NYU.

144. NYU's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because NYU is bound by industry standards to protect confidential PII.

145. NYU was subject to an "independent duty," untethered to any contract between NYU and Plaintiff or the Class.

146. NYU also had a duty to exercise appropriate clearinghouse practices to remove former students' and student-applicants' PII it was no longer required to retain pursuant to regulations.

147. NYU had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

148. NYU had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within NYU's possession might have been compromised, how it was compromised,

and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

149. NYU breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by NYU include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove former students' and student-applicants' PII it was no longer required to retain pursuant to regulations, and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

150. NYU violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. NYU's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

151. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statute was intended to guard against.

152. NYU's violation of Section 5 of the FTC Act constitutes negligence.

153. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

154. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of NYU's inadequate security practices.

155. It was foreseeable that NYU's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting educational institutions.

156. NYU has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

157. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. NYU knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on NYU's systems or transmitted through third party systems.

158. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

159. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, NYU's possession.

160. NYU was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

161. NYU's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the

actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

162. NYU has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

163. But for NYU's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

164. There is a close causal connection between NYU's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of NYU's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

165. As a direct and proximate result of NYU's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in NYU's possession and is subject to further unauthorized disclosures so long as NYU fails to undertake appropriate and adequate measures to protect the PII.

166. Additionally, as a direct and proximate result of NYU's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in

NYU's possession and is subject to further unauthorized disclosures so long as NYU fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

167. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

168. Plaintiff and Class Members are also entitled to injunctive relief requiring NYU to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

169. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

170. Plaintiff and Class Members were required deliver their PII to NYU as part of the process of applying for enrollment at NYU. Plaintiff and Class Members paid money, or money was paid on their behalf, to NYU in exchange for applying for enrollment and would not have paid for NYU's application, or would have paid less for them, had they known that NYU's data security practices were substandard.

171. NYU solicited, offered, and invited Class Members to provide their PII as part of NYU's regular business practices. Plaintiff and Class Members accepted NYU's offers and provided their PII to NYU.

172. NYU accepted possession of Plaintiff's and Class Members' PII for the purpose of providing enrollment services to Plaintiff and Class Members.

173. Plaintiff and the Class entrusted their PII to NYU. In so doing, Plaintiff and the Class entered into implied contracts with NYU by which NYU agreed to safeguard and protect such

information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

174. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that NYU's data security practices complied with relevant laws and regulations (including FTC guidelines on data security) and were consistent with industry standards.

175. Implicit in the agreement between Plaintiff and Class Members and the NYU to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

176. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and NYU, on the other, is demonstrated by their conduct and course of dealing.

177. On information and belief, at all relevant times NYU promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

178. On information and belief, NYU further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

179. Plaintiff and Class Members paid money to NYU with the reasonable belief and expectation that NYU would use part of its earnings to obtain adequate data security. NYU failed to do so.

180. Plaintiff and Class Members would not have entrusted their PII to NYU in the absence of the implied contract between them and NYU to keep their information reasonably secure.

181. Plaintiff and Class Members would not have entrusted their PII to NYU in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

182. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

183. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with NYU.

184. NYU breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

185. NYU breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and storage of other personal information after NYU knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

186. As a direct and proximate result of NYU's breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and

abuse; and (b) remains backed up in NYU's possession and is subject to further unauthorized disclosures so long as NYU fails to undertake appropriate and adequate measures to protect the PII.

187. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

188. Plaintiff and Class Members are also entitled to injunctive relief requiring NYU to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

189. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

190. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

191. Plaintiff and Class Members conferred a monetary benefit on NYU. Specifically, they paid NYU and/or its agents for enrollment applications and in so doing also provided NYU with their PII. In exchange, Plaintiff and Class Members should have received from NYU the enrollment services that were the subject of the transaction and should have had their PII protected with adequate data security.

192. NYU knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. NYU profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

193. NYU failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

194. NYU acquired the PII through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

195. If Plaintiff and Class Members had known that NYU would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at NYU or applied for enrollment at NYU.

196. Plaintiff and Class Members have no adequate remedy at law.

197. NYU enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, NYU instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of NYU's decision to prioritize its own profits over the requisite security and the safety of their PII.

198. Under the circumstances, it would be unjust for NYU to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

199. As a direct and proximate result of NYU's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in NYU's possession and is subject to further unauthorized disclosures so long as NYU fails to undertake appropriate and adequate measures to protect the PII.

200. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from NYU and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by NYU from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

201. Plaintiff and Class Members may not have an adequate remedy at law against NYU, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class Members, respectfully requests judgment against NYU and that the Court grant the following relief:

A. An Order certifying the Class and appointing Plaintiff and his Counsel to represent the Class;

B. Equitable relief enjoining NYU from engaging in the wrongful conduct alleged herein, including the misuse and/or disclosure of Plaintiff's and Class Members' Personally Identifiable Information (PII);

C. Injunctive and other equitable relief as necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order requiring NYU to:

i. Cease the wrongful and unlawful acts described herein;

ii. Implement appropriate security measures, including encryption, to protect all data collected in accordance with applicable laws, regulations, and industry standards;

iii. Delete, destroy, or purge Plaintiff's and Class Members' PII unless NYU can provide a compelling justification for its retention that outweighs their privacy interests;

iv. Reimburse out-of-pocket expenses incurred in the prevention, detection, and recovery from identity theft, tax fraud, and unauthorized use of PII for the lifetime of Plaintiff and Class Members;

v. Establish and maintain a comprehensive Information Security Program to safeguard the confidentiality and integrity of Plaintiff's and Class Members' PII;

vi. Prohibit the storage of Plaintiff's and Class Members' PII on cloud-based

databases without adequate security measures;

vii. Engage independent third-party security auditors and internal personnel to conduct periodic penetration testing, security audits, and risk assessments, with prompt remediation of any identified vulnerabilities;

viii. Implement automated security monitoring and conduct continuous security testing;

ix. Provide regular training for employees on security best practices and handling of PII, with additional training as necessary based on job responsibilities;

x. Segment data within its network to prevent widespread access in the event of a security breach;

xi. Conduct routine database scanning and security checks;

xii. Establish an information security training program, including mandatory annual training for all employees and additional specialized training as needed;

xiii. Develop and implement incident response protocols to ensure personnel can promptly identify, contain, and mitigate security breaches;

xiv. Implement a system for regularly testing employees' compliance with security policies and best practices;

xv. Maintain a threat management program to monitor internal and external security threats, ensuring tools are properly configured and regularly updated;

xvi. Provide comprehensive education to Class Members regarding the risks they face due to the compromise of their PII and the steps they must take to protect themselves;

xvii. Establish logging and monitoring programs to track and analyze traffic to and from NYU's servers; and

xviii. For a period of ten (10) years, retain an independent third-party assessor to conduct an annual SOC 2 Type 2 audit evaluating NYU's compliance with the Court's final judgment, with reports provided to the Court and Class Counsel, including disclosure of any deficiencies.

D. An award of damages, including actual, nominal, consequential, and punitive damages as permitted by law, in an amount to be determined;

E. An award of attorneys' fees, costs, and litigation expenses as permitted by law;

F. Prejudgment interest on all amounts awarded; and

G. Such other and further relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: March 26, 2025

Respectfully Submitted,

/s/ Katherine M. Aizpuru
Katherine M. Aizpuru (Bar No. 5305990)
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue, NW, Suite 1010
Washington, D.C. 20006
Phone: (202) 973-0900
kaizpuru@tzlegal.com

Sabita Soneji*
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, California 94612
Telephone: (510) 254-6808
ssoneji@tzlegal.com

Counsel for Plaintiff and Class

*Pro Hac Vice *application forthcoming*